8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,877	01/26/2001	Jeffrey Bruce Lotspiech	ARC92001005US1	6667

7590 06/29/2004

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary	**Application No.** 09/770,877	**Applicant(s)** LOTSPIECH ET AL.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61,65-88 and 95-97* is/are pending in the application.

4a) Of the above claim(s) *62-64 and 89-94* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☒ Claim(s) *7,9,12-16,18,20,27,29,32-35,38,40,47,49,52-55,58-60,68,70,73-75,80,82 and 85-87* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *2,3 and 4*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Continuation Sheet (PTOL-326) **Application No. 09/770,877**

Continuation of Disposition of Claims: Claims rejected are 1-6,8,10,11,17,19,21-26,28,30,31,36,37,39,41-46,48,50,51,56,57,61,65-67,69,71,72,76-79,81,83,84,88 and 95-97.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-61, 65-88 and 95-97 drawn to method for broadcast encryption and sending a session key, classified in class 713, subclass 163.

   II. Claims 62-64, drawn to system for storing data in a stateless receiver, classified in class 713, subclass 193.

   III. Claims 89-94, drawn to apparatus holding a message, classified in class 380, subclass 279.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions I, II and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as broadcasting data encryption using an encrypted session key, invention II has separate utility such as storing data in a stateless receiver, invention III has separate utility such as holding a message in a medium. See MPEP § 806.05(d).

3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for one group is not required for any other groups, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

6. During a telephone conversation with John L. Rogitz on June 8, 2004 a provisional election was made without traverse to prosecute the invention of group I, claims 1-61, 65-88 and 95-97. Affirmation of this election must be made by applicant in replying to this Office action. Claims 62-64 and 89-97 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Objections

7. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim 44 that depends on claim 43 has been renumbered 44a, and misnumbered claim 44 that depends on claim 41 has been renumbered 44b.

Applicant should renumber claims including the appropriate dependency.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 41 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "good" in claim 41 is a relative term which renders the claim indefinite. The term "good" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 1-6, 8, 10-11, 17, 19, 23-26, 28, 30-31, 36-37, 39, 41-46, 48, 50-51, 56-57, 61, 65-67, 69, 71-72, 76-79, 81, 83-84, 88, 95-97** are rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava, US Patent 6,684,331 in view of Aiello et al., US Patent 6,397,329.

a) **As to claims 1 and 41-42**, Srivastava discloses a method and apparatus for distributing and updating group controllers or multicast service agents over a wide area network based on a tree structure comprising assigning each user in a group of users respective private information I.sub.u which reads on private key (Fig. 2A, elements A-H; col. 2, lines 17-18); selecting at least one session encryption key K (col. 2, lines 37-41); encrypting the session key K, which reads on group key GK, with the subset keys L.sub.i1 to L.sub.im to render m encrypted versions of the session key K (Fig. 5). Srivastava discloses Diffie-Hellman protocol in Fig. 5, where subset keys reads on shared private key, however, it is well-known in the cryptography area that asymmetric algorithm is used to generate a ciphertext (col. 2, lines 1-8), wherein the sender encrypts the session key with the recipients public keys, which reads on the subset keys L.sub.i1 to L.sub.im. Srivastava does not teach partitioning users not in a revoked set R into disjoint subsets S.sub.i1 to S.sub.im having associated subset keys L.sub.i1 to L.sub.im.

Aiello discloses a method for revoking digital identities comprising partitioning users not in a revoked set R into disjoint subsets S.sub.i1 to S.sub.im having associated subset keys L.sub.i1 to L.sub.im (Fig. 6A and 6B).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of partitioning users not in a revoked set into disjoint subsets, as Aiello teaches, in the system of Srivastava, so as to provide a less expensive public key revocation scheme (col. 5, lines 56-59).

b) **As to claims 2-3, 23, 43-44a, 66 and 78**, Srivastava discloses the method further comprising partitioning the users into groups S.sub.1 to S.sub.w, wherein "w" is an integer, and the groups establish subtrees in a tree wherein the tree is a complete binary tree (Fig. 5).

c) **As to claims 4-5, 24-25 and 44b-45**, Srivastava discloses the method further comprising using private information I.sub.u to decrypte the session key (col. 16, lines 30-32). Srivastava discloses Diffie-Hellman protocol in Fig. 5, where subset keys reads on shared private key, however, it is well-known in the cryptography area that asymmetric algorithm is used to generate a ciphertext (col. 2, lines 1-8), wherein the sender encrypts the session key with the recipients public keys, which reads on the subset keys L.sub.i1 to L.sub.im. and the recipient decrypts the session key with the recipient's private key which reads on private information I.sub.u.

d) **As to claims 6, 26 and 46**, Srivastava discloses the method wherein each subset S.sub.i1 to S.sub.im includes all leaves in a subtree rooted at some node v.sub.i, at least each node in the subtree being associated with a respective subset key (Fig. 5, elements A-H, 507, 509, 511 and 513).

e) **As to claims 8, 28, 48, 69 and 81**, Srivastava discloses the method wherein each user must store log N keys, wherein N is the total number of users (col. 16, lines 17-19).

f) **As to claims 10, 30, 50, 71 and 83**, Srivastava discloses the method wherein the total number of users defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets. The revoked set R is a subset in the total number of users N, it is inherently understood that the same structure applied to the revoked set as well as to the total number of users.

g) **As to claims 11, 31, 51, 72 and 84**, Srivastava discloses the method wherein the tree includes a root (Fig. 5, element 501) and plural nodes (Fig. 5, elements 501, 503, 505, etc.), each node having at least one associated label (Fig. 5, elements 1, 2, etc.) and wherein each subset includes all leaves (Fig. 5, elements 11, A, B) in a subtree rooted at some node v.sub.i (Fig. 5, element 503) that are not in the subtree rooted at some other node v.sub.j (Fig. 5, element 509) that descends from v.sub.i.

h) **As to claims 17, 36-37, 56-57, 76 and 88**, the examiner takes official notice that use of pseudorandom sequence generator is quite well known in the data encryption art. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of pseudorandom sequence generator in the system of Srivastava so as to be cryptographically strong.

i) **As to claims 19 and 39**, Srivastava discloses the method wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each user is assigned keys from all nodes in a direct path between a leaf representing the user and the root (Fig. 5).

j) **As to claim 61**, see the above addressed claims 1, 2 and 11.

k) **As to claim 65 and 77**, see the above addressed claims 1 and 2.

l) **As to claims 67, 79 and 97**, Aiello discloses the receiver wherein subsets S.sub.i1 to S.sub.im derived from the set of groups S.sub.1 to S.sub.w define a cover (Fig. 6A and 6B).

m) **As to claims 95 and 96**, Aiello discloses the computer wherein the act of partitioning is undertaken by a system computer (Fig. 1, 5, 6A and 6B).

12. **Claims 21-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava, US Patent 6,684,331 in view of Aiello et al., US Patent 6,397,329 and further in view of Van Rijnsoever et al., US 2002/0090090.

a) **As to claim 21**, Srivastava discloses a computer program device (Fig. 8) comprising a computer program storage device including a program of instruction usable by a computer comprising logic means for accessing a tree to identify plural subset keys; logic means for encrypting a message with a session key; logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key (Fig. 5). Srivastava and Aiello do not teach logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers.

Van Rijnsoever discloses a transmission system where data is transmitted to a plurality of receivers and the encrypted session key is sent in a header of the message to plural receivers (page 2, paragraph [0017]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending the encrypted session key in the message header to plural receivers, as Van Rijnsoever teaches, in the system of Srivastava and Aiello, so as to provide conditional access to data services (page 2, paragraph [0017]).

b) **As to claim 22**, Srivastava discloses the computer program further comprising logic means for partitioning receivers not in a revoked set R into disjoint subsets S.sub.i1 to S.sub.im having associated subset keys L.sub.i1 to L.sub.im (Fig. 5).

Allowable Subject Matter

13. Claims 7, 9, 12-16, 18, 20, 27, 29, 32-35, 38, 40, 47, 49, 52-55, 58-60, 68, 70, 73-75, 80, 82, 85-87 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

a) US Patent 5,748,736 to Mittra discloses system and method for secure group communications via multicast or broadcast.

b) US Patent 6,629,243 to Kleinman et al. discloses secure communications system.

c) US Patent 6,247,127 to Vandergeest discloses method and apparatus for providing off-line communications.

d) US Patent 6,285,991 to Powar discloses secure interactive electronic account statement system.

e) On the Generation of Cryptographically Strong Pseudorandom Sequences, Adi Shamir, ACM Transactions on Computer Systems, vol. 1, no. 1, February 1983, pages 38-44.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
6/24/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100